Civil GPS Systems and Potential Vulnerabilities

Major David Hoey, *746th Test Squadron*
Paul Benshoof, *746th Test Squadron*

BIOGRAPHY

Major David Hoey is the Commander of the 746th Test Squadron. As such he oversees the Department of Defense's lead test organization in the GPS Test Center of Expertise, runs the Central Inertial Guidance Test Facility (CIGTF) and oversees the evaluation of both civil and military GPS systems' performance and vulnerability testing. He has previously held several positions in the Test and Evaluation community, principally dealing with avionics testing on a variety of US and Foreign aircraft. Maj Hoey is a 1996 Flight Test Engineering Graduate of the US Air Force Test Pilot School and also holds three degrees from the University of California, Davis, a MS and BS in Aeronautical Engineering and a BS in Mechanical Engineering

Mr. Paul Benshoof is the Director of the GPS Test Center of Expertise at the 746th Test Squadron. He has spent the last 14 years in GPS with duties that include leading the development and procurement of secure handheld GPS receivers for the Army; development of assets to support navigation warfare advanced technology demonstrations; and supervising international test programs for NATO and allied forces. Mr. Benshoof is a graduate of Syracuse University with a BS degree in computer engineering.

ABSTRACT

Since becoming fully operational, the Global Positioning System (GPS) has consistently proven itself as an effective force enhancer to the US military and its allies. However, because GPS satellites broadcast a signal freely available to the public, commercial applications of GPS outnumber those of the military by a wide margin and are now embedded in applications the original developers of GPS could have never imagined. Among these applications are those used in the United States' critical national infrastructure, which are becoming increasingly reliant on GPS at an alarming rate. Unfortunately, over-reliance on GPS for critical applications could leave us vulnerable to future asymmetric attacks. The danger stems from what is well understood in military circles: to function properly, GPS receivers must track low-power satellite signals which are very susceptible to jamming or other interference.

This paper presents a Department of Defense GPS test perspective on civilian GPS vulnerabilities and potential impacts to critical infrastructure, as well as recommends action to mitigate vulnerability exploitation and help protect vital applications.

OVERVIEW OF CIVIL GPS APPLICATIONS

Our national infrastructure has become dependent on GPS in several ways, many of which typically go unnoticed. Figure 1 shows many of the broad categories of GPS usage. The obvious applications center on navigation, which includes aviation, automobile, maritime, and rail control. GPS provides enhanced position and navigation accuracy that enables efficiency and safety on a large scale, in addition to advanced services such as stolen vehicle recovery. First responders, such as search and rescue teams and paramedics, are among the most visible users of GPS accuracy for critical public services.

Fig 1 Various GPS Applications

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
25-10-2005	Technical Report	To 50-10-2005

4. TITLE AND SUBTITLE
Civil GPS Systems and Potential Vulnerabilities

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Major David Hoey, 746th Test Squadron
Mr. Paul Benshoof, 746th Test Squadron

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

46th Test Group
872 DeZonia Road Bldg 1085
Holloman AFB, NM 88330-7714

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
46th Test Wing
Air Armament Center
Eglin AFB, FL 32542

10. SPONSOR/MONITOR'S ACRONYM(S)
AAC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for public release; distribution unlimited. AAC/PA09-01-05-348

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Since becoming fully operational, the Global Positioning System (GPS) has consistently proven itself as an effective force enhancer to the US military and its allies. However, because GPS satellites broadcast a signal freely available to the public, commercial applications of GPS outnumber those of the military by a wide margin and are now embedded in applications the original developers of GPS could have never imagined. Among these applications are those used in the United States' critical national infrastructure, which are becoming increasingly reliant on GPS at an alarming rate.

Unfortunately, over-reliance on GPS for critical applications could leave us vulnerable to future asymmetric attacks. The danger stems from what is well understood in military circles: to function properly, GPS receivers must track low-power satellite signals which are very susceptible to jamming or other interference.

This paper presents a Department of Defense GPS test perspective on civilian GPS vulnerabilities and potential impacts to critical infrastructure, as well as recommends action to mitigate vulnerability exploitation and help protect vital applications.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF: Unclassified			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	N/A	5	Kevin Dunshee
Unclassified	Unclassified	Unclassified			**19b. TELEPHONE NUMBER** *(include area code)* (505) 572-1227

However, GPS usage does not stop there. Some less obvious applications rely on the highly accurate GPS timing signal, which is an inexpensive alternative to costly, high maintenance timing equipment. Accordingly, the synchronization and management of major telecommunications networks are gravitating towards GPS reliance. This includes phones, pagers, wireless systems, and the Internet. GPS timing is also used in a number of other applications, as diverse as time-stamping electronic financial transactions to electrical power grid management and fault location.

Both the military and private sectors have played important roles in developing GPS technology and driving innovation. Originally, the U.S. government developed GPS as a three-dimensional all-weather navigation system that consolidated earlier Navy and Air Force navigation efforts. Since becoming fully operational, GPS has consistently been proven as an effective force enhancer to the U.S. military and our allies. GPS is now required on all U.S. systems and is a recognized NATO standard.

Because of this GPS reliance, the military has been at the forefront of developing the technology to preserve GPS services in an area of operation where enemy electronic interference is likely to be present. They have produced the solutions that make military navigation systems so much more robust than their civilian counterparts. Unfortunately, overall the military is a minority user of GPS by a wide margin, with current estimates at less than 1% of all known GPS applications, Figure 2.

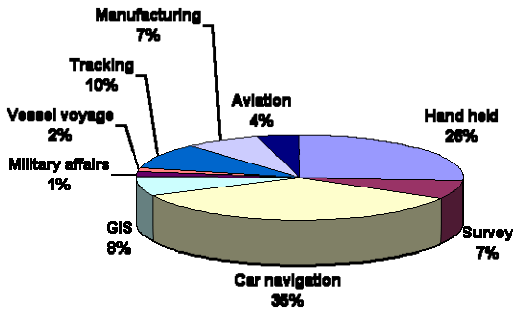


Fig 2 GPS Application Sectors

However, because GPS satellites broadcast a signal freely available to the public, commercial applications of GPS far exceed those of the military. This is where the real innovation is occurring. The private sector continues to use GPS in ways the original developers could have never imagined. Their innovations have profoundly affected the way we live, communicate, and travel, and new GPS applications are being introduced so often that it is clear this technology's utilization is nowhere near maturity.

On the day before the September 11th attacks, the Department of Transportation's Volpe Center released a report **[1]** assessing the vulnerability of the United States national transportation infrastructure relating to GPS. This report did an excellent job of examining potential vulnerabilities to civilian systems, and not just those pertaining to transportation. The report also addressed impacts to telecommunications and electronic finance. The danger stems from what the military has understood for years: GPS receivers derive their solutions from extremely low-power satellite signals, and these signals—like any radio transmission—can be jammed. Unfortunately, the worldwide use of GPS for military applications has driven the development of a "GPS Disruption Industry." GPS jamming techniques are no secret, simple plans for building jamming devices are readily available, and a number of them are available for purchase.

Fig 3 Russian GPS Jammer on the Open Market

Despite the Volpe Center's warnings about potential GPS vulnerabilities and the focus on domestic terrorism since the events of 9/11, the commercial use and reliance on GPS continues to increase. It's a bit disturbing but not too surprising. In fact, U.S. policy is to promote the acceptance and use of GPS as a world standard and to encourage private sector investment in the use of GPS technologies and services. Its low-cost and worldwide availability make it extremely attractive for all of its applications. However, recent world events have made us realize our civilian infrastructure is not invulnerable to enemy attack and we should therefore proactively identify these potential weaknesses and implement appropriate mitigation strategies.

A TEMPTING TARGET

GPS is an attractive technology that provides many benefits to our national infrastructure. However, as the Volpe Report points out, GPS is vulnerable to interference, and as this technology further penetrates the infrastructure it becomes a more tempting target to our adversaries. Accordingly, service providers and GPS users must be aware of these vulnerabilities and ensure that adequate independent backup systems or procedures are in place to be activated when needed.

With known vulnerabilities such as those outlined in the Volpe Report, one would like to think that commercial use would diminish, but in fact exactly the opposite is occurring. Commercial use is actually increasing, which is a bit alarming but not too surprising. US policy promotes acceptance of GPS as a low-cost, worldwide utility for commercial and military applications. However, we caveat this encouragement by stressing the civilian infrastructure is not invulnerable to enemy attack and ask that users proactively identify potential weaknesses and implement appropriate mitigation strategies.

In fact, six months before the Volpe Report was released, the Interagency GPS Executive Board, which has since become the National Position, Navigation, and Timing (PNT) Executive Committee, issued a statement **[2]** that reads "GPS provides many benefits to civilian users. It is vulnerable, however, to interference and other disruptions that can have harmful consequences. GPS users must ensure that adequate independent backup systems or procedures can be used when needed." We continue to stress this philosophy today.

GPS VULNERABILITIES DISCUSSION

GPS vulnerabilities can be exploited in three ways: through (1) unintentional interference, (2) intentional interference, and (3) human factors problems. Unintentional interference includes common radio frequency interference, ionospheric interference, and other interference relating to spectrum congestion. Intentional interference includes jamming and spoofing, or the broadcast of counterfeit signals. Human factors problems include user equipment limitations and GPS space vehicle anomalies, lack of user training, and general over-reliance on the technology.

To illustrate how weak GPS signals actually are, consider this analogy: a standard 100 watt light bulb is 10^{18} times more powerful than a GPS satellite signal at the receiver's antenna. As such, the jamming power required at a GPS receiver antenna need not be strong to be effective. In fact, in-band power on the order of a picowatt (10^{-12} watts) can cause interference. We know from recent conflicts and working closely with our allies that worldwide militaries already possess the ability to broadcast GPS jamming signals from existing military equipment, ranging from KWatt to MWatt output, which certainly exceeds the required picowatt of power. However, a common by-product of broadcasting at such high power is a significant electromagnetic signature that is easy to detect and locate, so these emitters are not considered a probable operational threat, at least not for very long.

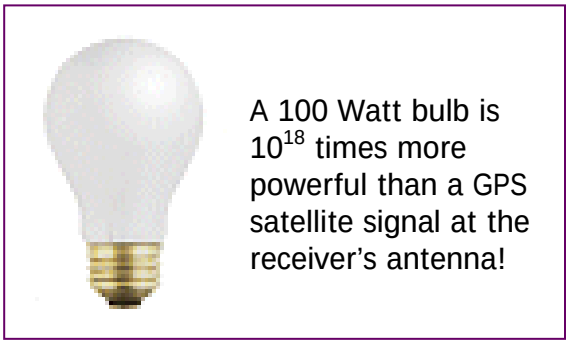


Figure 4 Example of GPS Low Power Signal

Instead, low power jammers, perhaps fewer than 100 watts, pose a potential persistent problem to GPS operations and are generally very affordable and easy to construct. These jammers can produce a number of potentially effective jamming signal types, including narrowband, broadband, and spread spectrum signals using pseudorandom noise modulation. Each signal type can affect different receivers in different ways, and if users do not know how their receivers respond to this interference, then they should consider investigating the effects to better understand their system limitations.

Of course, jamming by means of higher signal power is not the only way to potentially interfere with GPS. The fact that civilian GPS currently operates on a single frequency with a well-known signal structure affords the possibility of denying GPS accuracy through other potential disruption mechanisms. One technique, known as spoofing, involves the broadcast of a counterfeit GPS signal designed to provide false navigation information to the user. This technique is technically feasible, as the civilian C/A-code is short, well-known, and already widely available on a number of GPS signal generators. Another technique, referred to as meaconing, involves

capturing actual GPS transmissions and rebroadcasting them after a short delay. This technique could act similar to a spoofer without having to generate a false code. This interference strategy received renewed interest when a German company applied for a patent on the technique and consequently documented proposed employment scenarios.

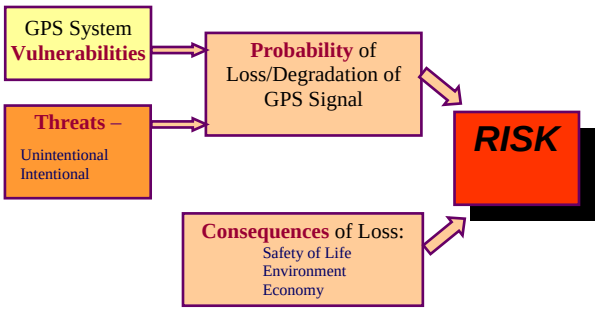
The possible effects of spoofing or meaconing are analogous to the effects of computer viruses, where a computer unknowingly processes malicious code and then demonstrates effects long after the virus transmission source is discontinued. As such, a GPS receiver could appear to be adversely affected long after a spoofer or meaconer has been actively broadcasting. Unfortunately for the civil GPS user, there is currently no off-the-shelf device that can protect a user from these possible effects.

Again, the military is leading the way when it comes to reducing vulnerabilities to their applications. Many government test organizations, including the 746th Test Squadron, have tested many of these technologies and have measured significant anti-jam protection, but so far little of it has transitioned into commercial applications. Some of the reasons for this relate directly to the GPS architecture that provides military users with an encrypted GPS signal offering increased anti-jam protection, but other reasons are cost-related. Many of the anti-jam solutions implemented by the military use specialized antenna electronics and hardware to reduce the effects of jammers, but the size and cost of these systems generally aren't considered practical for most commercial applications.

In the meantime, the U.S. Government is pursuing alternative solutions that will yield further improvements to anti-jam performance benefiting both military and civilian GPS users. Most significantly, the GPS Joint Program Office is working to modify the GPS architecture such that civilian users would have free access to three satellite signals. This will take some time to implement: the second signal won't be available before 2008, and the third is not expected before 2012. Also, the advent of microelectromechanical systems (MEMS) affords the possibility of embedding small inertial navigation sensors inside a GPS antenna to help improve a system's anti-jam performance. MEMS technology is not adequate to support this yet, but the cost, size, and performance of these devices continue to improve significantly. Government test organizations have been very active in evaluating MEMS technology for this type of application.

MITIGATION STRATEGIES

We know from previous discussion GPS has inherent vulnerabilities and there are threats, both intentional and unintentional, which can exploit these vulnerabilities. Considering the known vulnerabilities with the potential threats yields a probability of loss or degradation to a GPS signal to a particular application. Once this is known, one must weigh that probability against the consequences of the loss or degradation. This will establish a risk assessment, which if considered low may possibly be ignored. If it is considered high, then appropriate risk management techniques will need to be employed to reduce the risk to an appropriate level.



Source: John A. Volpe National Transportation Systems Center. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. 29 Aug 01

Figure 5 Risk Determination

The consequences of GPS signal loss or degradation will vary according to the application mode involved and the duration of the signal disruption. The impact of disruptions can be minimal if GPS accuracies can quickly be restored. However, longer outages could mean more severe impacts, including reduced operational effectiveness, economic damage, environmental concerns, and potential loss of life. When making such assessments, it is important to remember to consider the timing and synchronization advantages that GPS brings to non-navigation-related services such as communications and network applications, as they are often overlooked.

One way to mitigate over-reliance on GPS is to remember the technology is merely a tool to enhance response capabilities. Even the military, despite its reliance on GPS, recognizes that GPS is only one of many tools they use to do their job. Certainly, they have taken great strides to increase the probability this tool will always be available, but if they were denied GPS, they would still be prepared to accomplish their mission. First responders need to view GPS the same way. It is there to help you, but the success of your mission should not be directly

dependent on it without having appropriate backup procedures or systems.

It is also important to consider installing, or in some cases, continuing to maintain appropriate backup systems or procedures for each application. When designing backup systems, assess the potential interference impact in application designs and the feasibility of implementing systems to monitor, report, or locate interference sources. Some applications may be able to employ military anti-jam technology. Once backup systems are in place, encourage user training and use of these systems.

There are several organizations who can help you assess your system vulnerabilities and implement mitigation strategies. Members of the GPS Test Center of Expertise (COE) routinely offer this service to military organizations and have recently begun evaluating civil systems. Armed with years of military test experience and acute knowledge of how GPS receivers respond to various interference signals, these organizations are ideally suited to exploit the vulnerabilities of civilian GPS-based systems, assess the impact of the interference, and recommend the appropriate techniques to mitigate the unwanted effects.

JAMFEST is a specific opportunity offered by the Government to assist in evaluating potential vulnerabilities to GPS systems. It is a semi-annual event conducted by the 746th Test Squadron that delivers a low-cost realistic GPS jamming environment where users can test the vulnerability of their GPS-based systems or train their personnel in unique operational environments. Such an event gives anyone in need of GPS vulnerability awareness an avenue to test GPS assets in realistic jamming environments.

SUMMARY

Potential applications of GPS are vast and nowhere near maturity, with civilian use outnumbering military applications by a wide margin. Critical civilian systems increasingly rely on GPS, which presents the possibility of serious economic or fatal consequences if GPS signals are disrupted. As GPS continues to penetrate the civil infrastructure, it becomes a more tempting target for adversaries. Unfortunately, despite our advances in anti-jam solutions, this vulnerability will not be fully eliminated by technology alone. Other mitigation strategies will need to be employed smartly.

Balancing the benefits that technology offers against the vulnerabilities that it opens up begins with vulnerability awareness. When applying technology to a situation, one must determine how much risk he is willing to accept if that technology were to fail. In order to make that determination, one must study the associated vulnerabilities to determine tolerable levels of risk and cost for that application. Once risks and costs are identified, one can then apply appropriate risk management strategies to lower the system risk to an acceptable level.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the support of the GPS Joint Program Office, the Department of Transportation, and National PNT Executive Committee, and the 46th Test Group.

REFERENCES

1. *John A. Volpe National Transportation Systems Center. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. 29 Aug 01*

2. *Interagency GPS Executive Board. GPS Policy, Applications, Modernization, and International Cooperation. February 01*